CLAIMS

1. Process for controlling an Intranet network by means of a Web server, characterized in that it involves the steps of:

- discovering the devices of an Intranet network, including the different subnets;

- extracting data representative of those devices for the purpose of compiling a file which is transmitted through a HTTP protocol to said Web server;

- deploying a set of Internet Control Agents in the devices contained within said Intranet, said agent being controllable by a set of commands which are exchanged by means of the HTTP or HTTPS protocol;

thereby allowing the control of the Intranet by the Web server.

2. Process according to claim 1 characterised in that each Internet Control Agents regularly transmits a HTTP or HTTPS request to said server for the purpose of requesting a new set of instructions to be executed.

3. Process according to claim 1 characterised in that said set of instructions is used for controlling a remote installation of the software package within the devices.

4. Process according to claim 3 characterised in that said set of instructions is used for controlling an executable file for extracting technical data stored within the BIOS and the registry of the computers within the Intranet, said technical data being compiled in a text which is transmitted back to said server via a HTTP or HTTPS request.

5. Process according to claim 1 wherein said set of instructions includes an EXECUTE command for the purpose of executing a particular executable file located in a share resources, said EXECUTE command having a first parameter

defining the maximum time allowed to the execution and a second parameter defining the file where a report of the execution has to be created.

6. Process according to claim 1 wherein said set of instructions includes a DOWNLOAD command used for controlling said Internet Control Agent to download files connected in shared resources on the network.

7. Process according to claim 1 wherein said set of instructions includes a SLEEP command for scheduling the next execution of the Internet Control Agent for the purpose of the execution of a new set of commands or instructions.

8. Process according to claim 1 wherein said set of instructions includes a AUTO-UPDATE command used for controlling the update of the kernel of said Internet Control Agent installed within the considered device.

9. Process according to claim 1 characterised in that the installation of said Internet Control Agent in said computers operating under NT type environment is carried out by means of a NT service under control of a NT service control manager.

10. Process according to claim 9 wherein the installation successively involves the step of:

- installing an executable file for controlling a local setup procedure under the control of the NT service control manager (SCM) and in accordance with the description contained within a description file (*package.ini*) present on a shared resources; said executable file (*pushservice.exe*) receiving the format of a NT service;
- starting said executable file so as it becomes available to said computer as a service and permits the launching of a local setup procedure within said computer in accordance with the contents of said description file (*package.ini*).

11. Process according to claim 1 comprising a discovery mechanism based on the current IP address with a subnet mask being associated to the address of the router of the considered subnet, and using a PING for the purpose of discovering any active node within said subnet.

12. Process according to claim 11 wherein said detection of an active node is completed with a Simple Network Management Protocol (SNMP) for the purpose of determining the type of the device to be reported to said Web server.